# Remarks section:

This document explains why my patent is entirely different from Brustoloni, et al. patent number 6,963,982.

While Brustoloni patent is also trying to solve the NAT compatibility problem for certain protocols, e.g. IPsec, they take a very different route. They assume that the intermediate NAT devices can be modified. Our approach does not make that assumption.

They solve the NAT compatibility problem by:

a) Implementing an application layer gateways at the client
b) Obtaining the type of changes NAT device will make
c) Pre-compensating for those changes at the application layer gateway (ALG)

Our approach assumes that the NAT devices are not cooperative (which is the case in real life). We also do not require an application layer gateway (ALG). This means our solution will work on any application.

We solve the NAT compatibility problems by;

a) Duplicating the information on the sender side that is used by the received to observer the net effect of intermediate NATs. A lookup table is generated based on that information.

b) Reversing the effect of intermediate NATs on the packet based on the lookup table.

c) Using a gateway behind NAT to route packets to the end host and achieve true end-to-end secure communication. Brustoloni patent is completely lacking the concept of a gateway behind the NAT to solve the problem.

Another major problem with Brustoloni approach is that it cannot account for NAT at the receiver side. Our approach does not suffer from this problem as we reverse the effect of NAT on sender as well as the receiver side.

Unlike Brustoloni, our approach is practical and has been implemented in a product called, OmniVPN, that is commercially availbale from our website. www.trlokom.com

## Version with markings to show changes:

1. (Currently amended): A method for duplicating information in an IP packet with the ~~sole~~ intention of using it to partially or completely reverse the effect of intermediate NATs, comprising the steps of:

Identifying parts of an IP packet, including but not limited to the IP and transport layer headers, that can be potentially modified by NATs;

Copying that information into the packet in its current form or copying it into a different format;

Inserting ~~this~~the duplicate information into an IP packet after the IP and transport headers or appending it after the data portion of the packet in ~~a manner that keeps~~an encoded or original form to keep it protected from intermediate NATs.

2. (Currently amended): The method of claim 1 wherein complete IP header and the transport layer header is inserted into the IP packet~~. Such a~~ such that the transmitted packet will have duplicate IP and transport layer headers or a duplicate IP or transport layer header.

3. (Currently amended): The method of claim 1, wherein the duplicate information is inserted into the IP packets of the same connection ~~in a manner that keeps~~using a keyed or keyless encoding to keep it protected from intermediate NATs~~.~~ and recomputing the length and checksum fields in the IP and transport layer headers.

4. (Currently amended): The method of claim 1, wherein the duplicate information is inserted into the IP packets of a different connection~~. In addition,~~ and there are identifiers inserted into the IP packets of both connections to correlate ~~them.~~the information and observe the effect of intermediate NATs.

5. (Currently amended): A method for studying the effect of intermediate NATs with the ~~sole~~ purpose of using it to partially or completely reverse the effect of intermediate NATs, comprising the steps of:

Identifying parts of an IP packet, including but not limited to the transport and IP headers of the packet, that can be potentially modified by intermediate NATs;

Identifying parts of an IP packet from same or different connections that contain the original information~~-~~, including but not limited to the IP and transport layer headers, before intermediate NATs modified it;

Generating a look-up table that signifies the effect of intermediate NATs on the IP packets of that connection.

6. (Currently amended): A method for reversing partially or fully the effect of intermediate NATs based on a look-up table that signifies the effect of NATs on the IP packets of that connections. , comprising the steps of:

Modifying the body of the packet that may contain IP address or port numbers modified by intermediate NATs to their original values;

Modifying the transport header by replacing the original port numbers and recomputing part or all of the transport header as necessary;

Modifying the IP header the replacing the original source and destination IP address and recomputing the length and/or checksum.

7. (Currently amended): The method of claim 6 wherein only the effect of NAT on the transport layer header is reversed. by replacing the modified port numbers with the original ports numbers, adjusting the sequence and acknowledge numbers to correctly reflect the unmodified packet, and recomputing the checksum field.

8. (Currently amended): The method of claim 6 wherein only the effect of NAT on the IP header is reversed. by replacing the observed source and destination IP address with original source and destination IP addresses followed by recomputation the length and checksum.

9. (Currently amended): The method of claim 6 wherein the effect of NAT on the transport layer data is reversed. by reverting back to the original port numbers in the transport header, adjusting the sequence and acknowledge numbers if necessary, recomputing the checksum and length fields.

10. (Currently amended): A method for correcting the information in outgoing IP packets so that they arrive in a state expected by the NATs. comprising the steps of:

Modifying the transport header based on a lookup table so that the port numbers match that of the incoming network connection before the effect of the NAT were reversed;

Modifying the IP header based on a lookup table so that the source and destination IP addresses numbers match that of the incoming network connection before the effect of the NAT were reversed;

Modifying the message body based on a lookup table.

11. (Currently amended): The method of claim 10 where ~~the~~ IP header and/or the transport header of the outgoing packet is modified. by changing the destination and/or source IP headers of the packet based on a lookup table and recomputing the length, checksum, address, port number, sequence, and acknowledge number fields.

12. (Currently amended): The method of claim 10 where IP address or port number embedded inside the packet body ~~of the outgoing packet is~~are modified based on a lookup table and recomputing the length and/or checksum fields in the transport and/or IP headers.